UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA

v. **Case No. 8:03-CR-77-T-30TBM**

HATEM NAJI FARIZ
_____/

AMENDED MOTION FOR DISCLOSURE OF MATERIALS RELATED TO SURVEILLANCE PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT ("FISA") AND FOR SUPPRESSION OF THE FRUITS OF ALL SURVEILLANCE CONDUCTED UNDER FISA AND MEMORANDUM OF LAW IN SUPPORT

Defendant, Hatem Naji Fariz, by and through undersigned counsel, and pursuant to the First, Fourth, Fifth, and Sixth Amendments to the U.S. Constitution, 50 U.S.C. § 1806(e), (f), and (g), and Federal Rule of Criminal Procedure 12(b)(3)(C), respectfully requests that this Honorable Court (1) order the disclosure of materials related to surveillance of Mr. Fariz under the Foreign Intelligence Surveillance Act ("FISA") and (2) suppress the fruits of all surveillance under FISA. As grounds in support, Mr. Fariz states:

1. On February 25, 2003, the government filed its notice of intent to use information gathered from electronic surveillance pursuant to FISA during the trial and other proceedings against Mr. Fariz. (Doc. 26).

2. The government has informed the Court and defense counsel that this case invokes 152 applications for FISA wiretaps, and each of these applications essentially was three-month wiretap of the facility. (Doc. 89, Tr. 3/25/03, at 24). Mr. Fariz includes as the subject of this motion any and all FISA applications, orders, and intercepts where Mr. Fariz

is either the target or is overheard on others' surveillance. The government has indicated that it conducted wiretap surveillance of Mr. Fariz's phone line beginning in 2002 and continuing at least to the date of the original indictment in this case. *See, e.g.*, Affidavit of Kerry Myers in Support of Search Warrants 15 (Feb. 19, 2003). The government began its electronic surveillance of Sami Al-Arian and Ramadan Shallah in 1993 and 1994. *Id.* at 14-15. In 1999, the government began its electronic surveillance of Sameeh Hammoudeh in 1999. *Id.* Mr. Fariz has been recorded on others' wiretaps, including but not limited to Dr. Al-Arian and Mr. Hammoudeh, and the government has indicated that it will seek to introduce some of these statements at trial.

3. Counsel for Mr. Fariz have previously requested that the government disclose, *inter alia*, any FISA applications, court orders authorizing surveillance, and a copy of any minimization procedures. The government declined to produce any FISA materials in response to Mr. Fariz's general request and has failed to respond to Mr. Fariz's specific request for FISA materials.

4. Mr. Fariz herein seeks to suppress the fruits of any and all electronic surveillance conducted pursuant to FISA, under 50 U.S.C. § 1806(e) and the First and Fourth Amendments to the U.S. Constitution. Mr. Fariz first provides an overview of FISA. Second, Mr. Fariz requests the disclosure of the FISA related materials, pursuant to the Fifth and Sixth Amendments and 50 U.S.C. § 1806(f) and (g). If the Court denies this request for disclosure, Mr. Fariz would respectfully request the opportunity to submit a memorandum to assist this Court's *ex parte* review in its determination of the legality of the FISA

surveillance. Third, Mr. Fariz moves to suppress the fruits of all FISA electronic surveillance, pursuant to 50 U.S.C. § 1806(e). Finally, should the Court find that the FISA applications and orders comply with FISA, Mr. Fariz lastly moves to suppress the fruits of the FISA surveillance on the grounds that FISA itself is unconstitutional.[1] In order to fully address these issues, Mr. Fariz additionally requests an evidentiary hearing.

MEMORANDUM OF LAW

I. This Court Should Suppress All Fruits of Surveillance Under FISA, Based on Violations of the FISA Statute and the U.S. Constitution

Mr. Fariz is a United States citizen. He is therefore a United States person for purposes of FISA. 50 U.S.C. § 1801(i). Accordingly, Mr. Fariz is afforded not only the full protections of the First, Fourth, Fifth, and Sixth Amendments to the U.S. Constitution, but also additional protections under FISA, including that the FISA application may not be approved solely on the basis of First Amendment activities, that the application may not be based on clearly erroneous facts, and that the government must follow minimization requirements. 50 U.S.C. § 1801(h); *id.* § 1805(a)(3)(A); *id.* § 1805(a)(5).

A. Overview of FISA

Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, in 1978. Pursuant to FISA, a federal officer, with the approval of the Attorney General, may apply to the U.S. Foreign Intelligence Surveillance Court ("FISC") for an order approving

[1] Mr. Fariz has requested permission to file a separate memorandum in support addressing Mr. Fariz's constitutional arguments.

electronic surveillance made upon a belief that "the target of the electronic surveillance is a foreign power or an agent of a foreign power; and . . . each of the facilities or places at which the electronic surveillance is directed it being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(A), (B).[2] A "foreign power" means:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons; or
>
> (6) an entity that is directed and controlled by a foreign government or governments.

[2] FISA contains four parts, governing electronic surveillance (50 U.S.C. § 1801 *et seq.*), physical searches (50 U.S.C. § 1821 *et seq.*), register and trap and trace devices (50 U.S.C. § 1841 *et seq.*), and business records (50 U.S.C. § 1861 *et seq.*). As the government has only provided notice that "electronic surveillance" is at issue in this case, (Doc. 26), Mr. Fariz accordingly addresses the applicable provisions in FISA, 50 U.S.C. §§ 1801-1811.

50 U.S.C. § 1801(a).[3]

FISA defines an "agent of a foreign power" as any person who:

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

---

[3] "International terrorism," for FISA purposes, is defined as activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) appear to be intended--
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by assassination or kidnaping; *and*
(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

50 U.S.C. § 1801(c).

50 U.S.C. § 1801(b)(2).[4]

A FISA application must include, in addition to the statement of facts and circumstances justifying the officer's belief that the target is an agent of a foreign power, a certification from the Assistant to the President for National Security Affairs or an executive official designated by the President:

> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;[5]
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
>
> (E) including a statement of the basis for the certification that--
>
> > (I) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques;

---

[4] FISA also contains a definition of "agent of a foreign power" that pertains only to non-United States persons. 50 U.S.C. § 1801(b)(1). Since Mr. Fariz is a United States person, it does not apply here.

[5] Prior to the PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (Oct. 26, 2001), the executive officer was required to certify that "the purpose of the surveillance is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (2000). The PATRIOT Act amended this requirement to provide that the officer certify that "a significant purpose" of the surveillance is to obtain foreign intelligence information.

50 U.S.C. § 1804(a)(7)(A)-(E). FISA defines "foreign intelligence information" to mean:

> (1) information that relates to, *and if concerning a United States person is necessary to*, the ability of the United States to protect against--
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, *and if concerning a United States person is necessary to*--
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e)(1)-(2) (emphasis added). Finally, the application must also include, *inter alia*, (1) "a statement of the proposed minimization procedures," (2) "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance," (3) "statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance," and (4) "a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application." 50 U.S.C. § 1804(a)(5), (6), (8), and (9).

A judge of the FISC may approve an application for electronic surveillance if he finds, *inter alia*:

> (3) on the basis of the facts submitted by the applicant there is probable cause to believe that--
>
> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That *no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States*; and
>
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
>
> (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, *if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title*.

50 U.S.C. § 1805(a)(3)-(4) (emphasis added).

FISA provides than an "aggrieved person" may move to suppress evidence obtained or derived from such electronic surveillance if "(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval." 50 U.S.C. § 1806(e). An "aggrieved person" is defined as one "who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Mr. Fariz is an aggrieved person under FISA, both with respect to electronic surveillance where he is the target and where he is recorded in the course of others' FISA electronic surveillance. *United States v.*

Cavanaugh, 807 F.2d 787, 789 (9th Cir. 1987) (finding party to intercepted communication an aggrieved party); *United States v. Belfield*, 692 F.2d 141, 143, 146 n.21 (D.C. Cir. 1982) (finding that party "incidentally overheard during the course of surveillance of another target" is an aggrieved party); *see United States v. Badia*, 827 F.2d 1458, 1461 - 64 (11th Cir. 1987) (reviewing motion to suppress brought by individual heard on another's FISA surveillance).

B. Request for Disclosure

Mr. Fariz moves for disclosure of any and all FISA applications and orders where Mr. Fariz is the target of the proposed electronic surveillance, or where his conversations were otherwise subject to electronic surveillance under FISA. *See* 50 U.S.C. § 1801(k). Mr. Fariz anticipates that the government, as it has done in other cases involving FISA surveillance, will submit an affidavit of the Attorney General "under oath that disclosure or an adversary hearing would harm the national security of the United States," requiring this Court to review the FISA application, order, and other materials *in camera* and *ex parte*. 50 U.S.C. § 1806(f). The Court may, however, "disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance" or where "due process requires discovery or disclosure." *Id.* § 1806(f), (g). Mr. Fariz challenges any nondisclosure on both constitutional and statutory grounds.

Mr. Fariz first objects to the unfettered authority of the Attorney General to foreclose review of FISA applications, orders, and other materials by invoking the broad banner of "national security." As the Supreme Court has explained:

> It is fundamental that the great powers of Congress to conduct war and to regulate the Nation's foreign relations are subject to the constitutional requirements of due process. The imperative necessity for safeguarding these rights to procedural due process under the gravest of emergencies has existed throughout our constitutional history, for it is then, under the pressing exigencies of crisis, that there is the greatest temptation to dispense with fundamental constitutional guarantees which, it is feared, will inhibit governmental action. "The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers with the shield of its protection all classes of men, at all times, and under all circumstances."

Kennedy v. Mendoza-Martinez, 372 U.S. 144, 164-65 (1963) (footnote and citations omitted). FISA therefore cannot provide the Attorney General the authority to deny an individual due process by merely invoking national security concerns.

Instead, this Court should be provided the opportunity to decide, based on the circumstances of this particular case, whether disclosure is appropriate. Due process requires such an individualized determination. *See generally Matthews v. Eldridge*, 424 U.S. 319, 334-35 (1976) ("our prior decisions indicate that identification of the specific dictates of due process generally requires consideration of three distinct factors: First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute

procedural requirement would entail"); *see also Detroit Free Press v. Ashcroft*, 303 F.3d 683, 692 (6th Cir. 2002) (affirming ruling that government's "blanket closure of deportation hearings in 'special interest' cases [is] unconstitutional" under the First Amendment and indicating that "[w]hile we sympathize and share the Government's fear that dangerous information might be disclosed in some of these hearings, we feel that the ordinary process of determining whether closure is warranted on a case-by-case basis sufficiently addresses their concerns").

Otherwise, the government will always assert this privilege and deny any meaningful opportunity for review of its actions. Indeed, the defense is not aware of a single FISA case where the government did not assert a national security privilege. The government should not be provided the unchecked authority to deny access to the defense of the FISA applications and orders, since such denial violates Mr. Fariz's due process right to be heard at a meaningful time and in a meaningful manner under the Fifth Amendment, *see Matthews*, 424 U.S. at 333, and denies him the opportunity to be provided the effective assistance of counsel, guaranteed to him by the Sixth Amendment.[6] In the absence of disclosure, counsel

[6] While Mr. Fariz recognizes that other courts have upheld the automatic *ex parte*, *in camera* review upon the filing of the Attorney General's affidavit against constitutional challenges, Mr. Fariz notes that the Eleventh Circuit apparently has not addressed the constitutionality of 18 U.S.C. § 1806(f). *See Badia*, 827 F.2d at 1464 (examining whether disclosure was required under the statutory language of FISA). Moreover, as next addressed, even if this provision is constitutional, courts have recognized situations in which FISA disclosure may be appropriate. Mr. Fariz asserts that this is such a case.

for Mr. Fariz are left to guess the bases for the FISA applications, undermining any opportunity for meaningful review of the government's actions in this case.

In addition, Mr. Fariz contends that disclosure of the requested FISA materials, in this particular case, is warranted under 50 U.S.C. § 1806(f) and (g), as disclosure is necessary to ensure an accurate determination of the legality of the surveillance and is required under due process. Courts have recognized that *ex parte*, *in camera* review may not be appropriate where the case is complex. *Cf. Badia*, 927 F.2d at 1464 (noting that "the district court was able to determine the legality of the [FISA] surveillance without disclosing the contents of the application"); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990) ("the Court finds that the issues in this case are not so complex that the participation of the defendant is required to accurately determine the legality of the [FISA] surveillance at issue"); *In re Matter of Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985) ("The [FISA] applications are not lengthy nor are the orders. All are straightforward and readily understood and I perceive no necessity for assistance in the form of counsel's analysis or argument. The issues here are few and well defined and do not require any extensive investigation as in *Alderman v. United States*, 394 U.S. 165, 89 S. Ct. 961, 22 L. Ed. 2d 176 (1969)."); *see also United States v. Lemonakis*, 485 F.2d 941, 963 (D.D.C. 1973) (noting that in that case "the task of ascertaining relevance is *not* 'too complex, and the margin of error too great, to rely wholly on the *in camera* judgment' of this court" in its CIPA review) (citation omitted).

The Supreme Court's observations in *Alderman v. United States*, 394 U.S. 165 (1969), in this regard are particularly instructive:

> Adversary proceedings are a major aspect of our system of criminal justice. Their superiority as a means for attaining justice in a given case is nowhere more evident than in those cases, such as the ones at bar, where an issue must be decided on the basis of a large volume of factual materials, and after consideration of the many and subtle interrelationships which may exist among the facts reflected by these records. As the need for adversary inquiry is increased by the complexity of the issues presented for adjudication, and by the consequent inadequacy of ex parte procedures as a means for their accurate resolution, the displacement of well-informed advocacy necessarily becomes less justifiable.
>
> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands.

Id. at 183-84. Mr. Fariz submits that the complexity and volume of the alleged facts, individuals involved, and the interrelationships between them requires the participation of defense counsel for this Court to be assured of an accurate determination of the legality of the FISA electronic surveillance in this case.

In addition to the criteria for disclosure contained in 50 U.S.C. § 1806(f), courts have examined the legislative history and found:

> The legislative history explains that such disclosure is "necessary" only where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as "indications of possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order."

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701 at 64 (1978)); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984). As explained more fully in Part C, *infra*, Mr. Fariz submits at a minimum that he should be provided the applicable FISA materials under this standard, particularly in light of the "significant amount of nonforeign intelligence information" contained in the FISA intercepts, "calling into question compliance with the minimization standards contained in the order." *Id.*

C. Compliance with FISA

Mr. Fariz challenges the government's compliance with the statutory requirements of FISA. Should the Court decide to review the FISA applications, orders, and other materials *ex parte* and *in camera*, Mr. Fariz submits the following outline of issues for the Court's consideration and would respectfully request the opportunity to provide a memorandum *ex parte* to brief these issues more fully. While the government must meet each of the requirements of FISA, Mr. Fariz focuses on the significant issues that will likely be involved in the review of the FISA materials.

1. "Agent of a foreign power," the First Amendment, and Clearly Erroneous Facts

Mr. Fariz challenges whether the government could demonstrate that he was an "agent of a foreign power," as defined in 50 U.S.C. § 1801(b)(2). Of the criteria, only one seems likely to have been relied upon (based on the charges in this case): any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power," or knowingly aids and abets or knowingly

conspires to do so. 50 U.S.C. § 1801(b)(2)(C), (E). "International terrorism," by its FISA definition, involves violent acts or acts dangerous to human life. 50 U.S.C. § 1801(c)(1) (including as one of the required factors that the activities "involve violent acts or acts dangerous to human life . . .").

Mr. Fariz asserts that the government could not meet this standard when it submitted its FISA application(s) with respect to Mr. Fariz. For example, the government concedes that the Defendants in this case, including Mr. Fariz, have not participated in any violent acts themselves, nor has there been any allegations against Mr. Fariz that he planned or engaged in activities in preparation for any attacks. Moreover, for the government to have proceeded under an aiding and abetting or conspiracy theory, the government would have had to show that Mr. Fariz had the intention of furthering the violent acts. As such, Mr. Fariz contends that he does not meet the definition of an "agent of a foreign power." *See Badia*, 827 F.2d at 1461,1464 ("The documents show clearly that Arocena was an agent of a foreign power as defined by § 1801(b)(2)(c)). Specific facts in the application establish that Arocena had participated in terrorist acts on behalf of Omega-7 [a militant anti-Castro organization], and had been actively engaged in international terrorism prior to the date of the publication for surveillance.").

The FISA application must additionally go beyond activities protected by the First Amendment in order to comply with the requirements of FISA. For example, the FISA application cannot be based on mere association with other individuals or groups – not only because it would not meet the definition of "agent of a foreign power," but also because such

activities would be protected by the First Amendment.[7] Additionally, for any fund-raising to be the basis of a claim that Mr. Fariz was an "agent of a foreign power," Mr. Fariz contends that the government would have had to demonstrate, based on facts that were not clearly erroneous, that he intended that these funds would go toward violent attacks. Mr. Fariz bases this contention not only on long-standing Supreme Court precedent, but on the statutory language contained in FISA. 50 U.S.C. § 1801(b)(2); *id.* § 1801(c); *see, e.g., NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 916-17 (1982); *Healy v. James*, 408 U.S. 169, 186 (1972); *Scales v. United States*, 367 U.S. 203, 229 (1961) (citing *Noto v. United States*, 367 U.S. 290 (1961)).

In the absence of disclosure of the FISA applications, it is difficult to address any inaccuracies regarding the basis of whether Mr. Fariz was an agent of a foreign power in detail. Mr. Fariz at this juncture would note that to the extent that any of the FISA applications or renewal applications relied on alleged conversations between Mr. Fariz and Abd Al Aziz Awda or about Awda, as described in the original indictment's Overt Acts 236, 238, 240, and 247, the government has admitted that Awda was misidentified. In this respect, such an application would be based on facts that were "clearly erroneous." 50 U.S.C. § 1805(a)(5). Moreover, the government had information as early as 2000 that Awda had left the PIJ to join the Palestinian Authority ("PA"), and had information in 1998 that

[7] Mr. Fariz incorporates by reference his First and Fifth Amendment arguments made in his Response to the Government's Motion for Reconsideration of the Court's March 12, 2004 Order As it Pertains to the Science Requirements of a Section 2339B Prosecution. (Doc. 543).

Awda was part of a splinter group that advocated improving relations with the PA. (Doc. 683). If any of the FISA applications relied on a connection between Awda and PIJ to justify surveillance but omitted this information, this omission would be material and would require further consideration, and possible suppression, pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978).

2. Purpose of the Surveillance: Whether to Obtain Foreign Intelligence Information

For FISA electronic surveillance prior to October 26, 2001, the appropriate executive official had to certify that "the purpose of the surveillance is to obtain foreign intelligence information." Beginning on October 26, 2001, Congress amended this provision to require that "a significant purpose" of the surveillance be to obtain foreign intelligence information. Mr. Fariz seeks disclosure, or at least Court review, of government records relating to the purpose of the electronic surveillance in this case, those responsible for overseeing and directing the surveillance, when such information was shared between intelligence officials and law enforcement personnel, and the FISA applications and orders providing such information. Only by review of these documents can Mr. Fariz be assured that the government complied with this requirement of FISA. *See, e.g., Badia*, 827 F.2d at 1464 (finding that "the documents establish that the telephone surveillance of Arocena did not have as its purpose the primary objective of investigating a criminal act.").[8]

[8] Mr. Fariz recognizes that the U.S. Foreign Intelligence Surveillance Court of Review, in its first ever appeal, disagreed with other courts of appeals that had held that FISA required that obtaining foreign intelligence information be the "primary purpose" of the electronic surveillance.

In particular, Mr. Fariz questions when the investigation became primarily criminal in nature. As early as November 1995, the government obtained criminal search warrants of Dr. Al-Arian's residence, Dr. Al-Arian's office at the University of South Florida, and the Office of the World Islamic Studies Enterprise, based on an investigation "of possible criminal conduct by Sami Al-Arian, Ramadan Abdullah Shallah, the Islamic Committee for Palestine, also known as the Islamic Concern Project . . ., the World Islamic Studies Enterprise . . ., and persons and entities association with them." Affidavit of William D. West at 2 (M.D. Fla. Nov. 17, 1995). In December 1995, FBI Special Agent Barry Carmody sought another criminal search warrant and reported that the government had seized from the residence of Dr. Al-Arian "a letter written by Sami Al-Arian in which Al-Arian is soliciting funds for the Islamic movement in Palestine . . . . This letter also appeals for support for the Jihad so that the people will not lose faith in Islam. As noted previously, the Jihad has been declared an international terrorist organization by the Department of State." Application and Affidavit for Search Warrant of M. Barry Carmody, Case No. 95-529-MM, at 4 (M.D. Fla. Dec. 19, 1995). Accordingly, at least by November 1995, the government was pursuing its criminal investigation of Dr. Al-Arian and others, based on activities that the government is now using to support its charges under RICO.

See In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intel. Surveillance Court 2002). Mr. Fariz addresses this issue along with his constitutional challenge to the appropriateness of FISA electronic surveillance in a separate memorandum of law.

Mr. Fariz would further request disclosure, or at least Court review, of the dates of any and all federal grand jury activity in this matter. Mr. Fariz reasons that since his surveillance began in 2002 and continued until the date of the indictment, the FISA application and renewal applications must have been submitted to the FISC at the latest during and periodically through 2002. The original indictment in this case, containing 50 counts and 121-pages, was returned on February 19, 2003. (Doc. 1). Mr. Fariz requests information concerning when the government began to seek an indictment against the Defendants and whether there is an overlap in activity. Mr. Fariz additionally requests any and all authorizations of the Attorney General referenced in 50 U.S.C. § 1806(b). *See In re Kevork*, 634 F. Supp. at 1007 (noting that the Attorney General authorizations approving the use of FISA intercepts in the proceedings have been made available to the defendants).

3. The Information Cannot Reasonably Be Obtained by Normal Investigative Techniques

Mr. Fariz challenges whether the information that the government sought could not have been obtained through normal investigative techniques, including a Title III wiretap. *See* 50 U.S.C. § 1804(a)(7)(C). Mr. Fariz notes that many of the offenses alleged in this case are included in the list of offenses for which wiretapping can occur under Title III. *See* 18 U.S.C. § 2516; 18 U.S.C. § 2518; *see also* U.S. PATRIOT Act, Pub L. No. 107-56, § 201, 115 Stat. 272, 278 (2001). That Congress included these crimes in Title III demonstrates that Congress intended for Title III to remain the mechanism for law enforcement to conduct surveillance for terrorism-related criminal investigations. If the government could not have

met the standards for a Title III wiretap, namely probable cause that one of the enumerated crimes was being committed, FISA was not designed to be an end-run around the Fourth Amendment warrant requirement.[9] The government has informed the Court that all of the intercepts listed in the original indictment were obtained through FISA, not Title III. (Doc. 89, Tr. 3/25/03, at 24-25). At some point, as addressed in Part C.2, *supra*, the government had to have shifted its focus to a criminal investigation. Mr. Fariz therefore challenges whether the government has met this FISA requirement.

4. Minimization Procedures

FISA requires that an order approving electronic surveillance must be based on a finding that "the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title." 50 U.S.C. § 1805(a)(4). "Minimization procedures" are defined as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, *to minimize the acquisition and retention, and prohibit the dissemination*, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, *which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent*, unless such person's identity is

---

[9] This concern is not trivial. In 2003, FISA wiretap applications exceeded requests for Title III wiretaps by federal and state authorities combined. *See* Rebecca Carr, *Terror Wiretaps Exceed Criminal Wiretaps for First Time*, Palm Beach Post (May 10, 2004). Mr. Fariz addresses this issue more fully in his memorandum of law in support of his constitutional arguments.

> necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information *that is evidence of a crime* which has been, is being, or is about to be committed and *that is to be retained or disseminated for law enforcement purposes*; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

50 U.S.C. § 1801(h) (emphases added).

The minimization procedures used in the FISA electronic surveillance applicable in this case should have been included within the FISA applications and orders, and therefore Mr. Fariz requests disclosure of these materials. Mr. Fariz further submits that real questions exist as to whether the government followed the minimization procedures in this case, as defined in 50 U.S.C. § 1801(h), providing an additional basis for the disclosure of these materials and suppression.

Minimization procedures are designed "to protect the privacy rights of Americans," *In re All Matters*, 218 F. Supp. 2d 611, 613 (FISC 2002). The manner in which the FISA electronic surveillance was conducted in this case failed to secure Mr. Fariz's privacy rights as an American, and cannot be justified based on either foreign intelligence or law enforcement purposes. *See* 50 U.S.C. § 1801(h). With respect to "acquisition," every telephone conversation was subject to monitoring during Mr. Fariz's own wiretap in 2002,

and every call on Dr. Al-Arian's phone lines over approximately a ten-year period and Mr. Hammoudeh's phone lines over a four-year period were as well. The government recorded, and thus retained, by its own estimates approximately 21,000 hours (or 2.4 years) of conversations. Even though the FISC has provided wide latitude with respect to retention in light of the nature of the information sought (*see In re All Matters*), the length and extent of the monitoring and retention of these conversations cannot be justified under an appropriate minimization procedure.

Indeed, Mr. Fariz challenges whether the procedures used in this case properly complied with the requirements of 50 U.S.C. § 1801(h). According to the FISC, the government has been following Standard Minimization Procedures for a U.S. Person Agents of Foreign Powers that were promulgated in July 1995, augmented in 2001, and approved by the FISC. *See* 218 F. Supp. 2d at 615, 616. Under these procedures, the following steps are taken in the minimization process:

> • information is reduced to an intelligible form: if recorded it is transcribed, if in a foreign language it is translated, if in electronic or computer storage it is accessed and printed, if in code it is decrypted and if on film or similar media it is developed and printed;
> • once the information is understandable, a reviewing official, usually an FBI case agent, makes an informed judgment as to whether the information seized is or might be foreign intelligence information related to clandestine intelligence activities or international terrorism;
> • if the information is determined to be, or might be, foreign intelligence, it is logged into the FBI's records and filed in a variety of storage systems from which it can be retrieved for analysis, for counterintelligence investigations or operations, or for use at criminal trial;
> • if found not to be foreign intelligence information, it must be minimized, which can be done in variety of ways depending upon the format of the information: if recorded the information would not be indexed, and thus

> become non-retrievable, if in hard copy from facsimile intercept or computer print-out it should be discarded, if on re-recordable media it could be erased, or if too bulky or too sensitive, it might be destroyed.

Id. at 617-18. Additionally, those "communications of or concerning United States persons *that could not be* foreign intelligence information or are not evidence of a crime . . . may not be logged or summarized." *Id.* at 618 (quoting Standard Minimization Procedures for U.S. Person Agent of a Foreign Power in Section 3.(a)(4) Acquisition/Interception/Monitoring and Logging) (emphasis in original). Further, according to 18 U.S.C. § 1801(h)(2), such information should not be disseminated without the U.S. person's consent.

At the very least, private conversations wholly irrelevant to either foreign intelligence or law enforcement were shared between intelligence officials and law enforcement officials in this case, in violation of 18 U.S.C. § 1801(h)(2) and (3).[10] The U.S. Attorney's Office has admitted that the vast majority of the 21,000 hours it was provided are irrelevant to the crimes alleged in this case. *See, e.g.*, Doc. 461, Tr. 1/22/04, at 61-72; Doc. 648, Government's Response, at 5 (indicating that fewer than 40 conversations involving Mr. Fariz were included in the Superseding Indictment). Accordingly, with respect to such calls involving or concerning Mr. Fariz, such calls were disseminated to law enforcement

[10] As an illustration, the U.S. Attorney's Office has provided to the defense approximately 1,500 CDs containing FISA intercepts, in addition to the cassette tapes containing the calls alleged in the original indictment. The very first conversation that the undersigned heard on a CD was a conversation in English, clearly not involving any of the Defendants in this case (based on the voices and accents of the participants), between a man and a woman concerning what appeared to be their extramarital affair. Such conversations were not properly disseminated to the U.S. Attorney's Office pursuant to any minimization procedure under 50 U.S.C. § 1801(h)(2) and (3).

personnel, without his consent, in violation of FISA. 50 U.S.C. § 1801(h)(2) (providing that "nonpublicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner that identifies any United States person, without such person's consent."). Moreover, if the information was not "evidence of a crime," it should not have been provided to law enforcement. 50 U.S.C. § 1801(h)(3).

In this respect, the application and orders of FISA in this case failed to comply with Congress's intent that "*rigorous and strict controls* be placed on the retrieval of such identifiable information and its dissemination or use *for purposes other than counterintelligence or counter terrorism*." *In re All Matters*, 218 F. Supp. 2d at 618 (quoting H.R. Rep. 95-1283, at 59 (1978)) (emphasis in original). The wholesale dissemination of Mr. Fariz's and others' private conversations, irrelevant to either foreign intelligence or law enforcement, was certainly not "rigorous" or "controlled." Mr. Fariz therefore contends that the FISA surveillance should be suppressed for noncompliance with the FISA minimization requirements.

D. Constitutional Arguments

Should the Court determine that the FISA applications and orders comply with the requirements of FISA for electronic surveillance, Mr. Fariz also challenges the electronic surveillance based on violations of the U.S. Constitution. Mr. Fariz addresses these issues in a separate memorandum of law.

E. Conclusion

Based on the foregoing, Mr. Fariz requests that this Court (1) order the disclosure of the FISA orders, applications, and materials and (2) suppress the fruits of all FISA surveillance in this case.

Respectfully submitted,

R. FLETCHER PEACOCK
FEDERAL PUBLIC DEFENDER

/s/ M. Allison Guagliardo

M. Allison Guagliardo
Florida Bar No. 0800031
Assistant Federal Public Defender
400 North Tampa Street, Suite 2700
Tampa, Florida 33602
Telephone: 813-228-2715
Facsimile: 813-228-2562
Attorney for Defendant Fariz

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 23rd day of November, 2004, a true and correct copy of the foregoing has been furnished by CM/ECF, to Walter Furr, Assistant United States Attorney; Terry Zitek, Assistant United States Attorney; Cherie L. Krigsman, Trial Attorney, U.S. Department of Justice; William Moffitt and Linda Moreno, counsel for Sami Amin Al-Arian; Bruce Howie, counsel for Ghassan Ballut; and to Stephen N. Bernstein, counsel for Sameeh Hammoudeh.

/s/ M. Allison Guagliardo
M. Allison Guagliardo
Assistant Federal Public Defender